Data Protection Policy

Stichting Dorcas Aid International

Version: 16.3 (definite)

Contents

1. Context and overview

1.1 Key details

- Policy prepared by: Nico Hoogenraad
- Approved by MT on: January 30th, 2017
- Policy became operational on: April 2st, 2017
- Next review date: June 30th, 2019

1.2 Introduction

Dorcas needs to gather and use certain information about individuals. These can include supporters, beneficiaries, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the organization's data protection standards – and to comply with the law.

1.3 Why this policy exists

This data protection policy ensures that Dorcas:

- Complies with data protection law and follow good practice
- Protects the rights of staff, beneficiaries, customers and partners
- Is open about how it stores and processes individuals' data
- Protect itself from the risks of a data breach

1.4 Data protection law

In the Dutch setting, there are a few laws and institutions we have to reckon with:

1.4.1. Law on protection of personal information

The 'Wet Bescherming Persoonsgegevens (Wbp)' lays the framework how organizations have to protect the information of third parties that they keep in the context of their 'business'. In order to prevent data loss, organizations need to protect the information by taking technical and organizational measurements. They have to use modern techniques to protect personal information, while also how the organization handles this information, like who has access to the information?

Organizations are required to think about the safety of the information beforehand, before they will start collecting data, but it also needs continual attention within the organization to keep it up-to-date and sufficient for the development of technology.

Some of the areas of attention in this law are:

- Processing where necessary;
- Confidentiality
- Security in-house
- Security when processed by third parties
- Measurements in a plan-do-check-act cycle
- Measurements based on risk analysis
- Measurements based on security standards

- Measurements based on processing by third parties
- Agreements for processing by third parties
- Oversight over compliance to agreements
- Reliability requirements
- Evaluation and adjustments

1.4.2. Law on notification data leaks

Since January 1st, 2016, the 'Wet Melding Datalekken' is applicable. This law stipulates that each organization has to notify the 'Authority Personal Information' as soon as it has become clear that there has been a serious data leak from the information they keep on personal information of individual people and or organizations.

A data leak is defined as access, destruction, modification or release of personal information from an organization, without it being the intention of the organization. Also unlawful processing is considered to be a data leak. We have to speak of a data leak if there has been a breach on the security of personal information as explained in article 13 of the Law on protection of personal information. With a data leak personal information has been subject to loss or illegal processing – to those things for which security measures should have prevented. This includes loss of USB sticks, a stolen laptop or unwanted access in data files by a hacker.

1.4.3. Authority Personal information

The 'Autoriteit Persoonsgegevens' supervises compliance of privacy legislation on registration of personal information. The authority investigates the developments, advises on new legislation, informs the public on rules an regulations and receives and processes tips on breaches of legislation, on which they can launch specific investigations.

Next to these, organizations that have discovered data leaks have to report these to the Authority by means of a fixed procedure.

2. People, risks and responsibilities

2.1 Policy scope

This policy applies to:

- Dorcas headquarters in the Netherlands
- All branches of Dorcas, known as 'field offices'
- All legal entities in other countries that de facto operate as Dorcas field offices
- All DFO's (Dorcas Fundraising Organizations) in countries where the prime activity for Dorcas is fundraising and not implementing projects
- All Dorcas staff and volunteers
- All contractors, suppliers and other people working on behalf of Dorcas that get to work with the data that Dorcas holds

It applies to all data that Dorcas holds relating to identifiable individuals, companies and organizations, even if that information technically falls outside of the 'Wet Bescherming Persoonsgegevens'. This data can include:

- Names of individuals
- Postal and physical addresses
- Email addresses
- Telephone numbers
- Donation information
- Way of involvement with Dorcas
- Plus any other information relating to individuals, companies and organizations

2.2 Data protection risks

This policy helps to protect Dorcas from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how Dorcas uses data relating to them, whether to receive direct mailing and how many times.
- **Theft.** For instance, information unlawfully obtained by third parties like hackers, which can be used for alternate objectives.
- **Reputational damage.** For instance, Dorcas will suffer if sensitive data becomes available in ways and manners in which Dorcas did not intend to have it become available.

2.3. Responsibilities

Everyone who works for or with Dorcas has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that Dorcas meets its legal obligations.
- The **director of finance and supporting services** also functions as the data protection officer, and is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies annually.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Checking and approving any contracts or agreements with third parties that may handle Dorcas' sensitive data.
- The **ICT coordinator** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data, for instance cloud computing services.

- The **Country Directors** are responsible for dealing with ICT and data-protection within the sphere of the Dorcas field offices, as concerning to local donors, beneficiaries, staff and other parties, especially where it pertains to individual information that Dorcas obtains from beneficiaries to be used within its programmes.
- The **team leader Backoffice** is responsible for dealing with requests from individuals to see the data Dorcas holds about them (also called 'subject access requests').
- The **team leader MarCom**is responsible for:
  - Approving any data protection statements attached to communications such as e-mails or letters or expressed in direct marketing letters, news magazines or online marketing.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

3. General staff guidelines

1. The only people able to access data covered by this policy should be those who **need it for their work.**
2. Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line managers.
3. **Dorcas will provide training** to all employees to help them understand their responsibilities when handling data.
4. Employees should **keep data secure**, by taking sensible precautions and following the guidelines in this policy.
5. In particular, **strong passwords must be used** and they should never be shared. All passwords to the computer network, intranet, CRM, Cobra, Twinfield and other (cloud) software solutions should be changed regularly and compulsory, depending on the possible exposure that unauthorized password usage brings about.
6. Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
7. Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
8. Employees **should request help** from their line manager or the finance director if they are unsure about any aspect of data protection.

4. Data storage

These rules describe how and where data should be stored safely. Questions about storing data safely can be directed to the IT manager or the finance director.

When data is **stored on paper**, it should be kept in a secure place where unauthorized people cannot access it. These guidelines also apply to data that is usually stored electronically, but has been printed out for some reason:

- When not required, the paper of files should be kept in **a locked drawer or filing cabinet.**
- Employees and volunteers should make sure paper and printouts are **not left where unauthorized people can access them**, like on or near a printer. (In this context, it is important that volunteers working with these data will get the same instruction and same training as employees.)
- **Data printouts should be shredded** and disposed of securely when no longer required. This can be done either with the help of some shredders in the offices, or at HQ – especially when it concerns large quantities - by depositing it in the container that is available just before the Dorcas Shop entrance. The contents of this container will be shredded by a third party.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never, ever shared between employees. Where temporary employees take over tasks from regular employees, they should have their own passwords and not use the passwords from the regular employees.
- If data is **stored on removable media** (like a CD, DVD, USB stick, laptop or portable hard drive, these should be kept locked away securely when not being used. When necessary transport has to take place, utmost care should be taken they are not left behind in a car or other public places where others can take the removable media or access them unauthorized. The one transporting the media should at all times keep them with himself or store them safely at his or her residence.
- Data should only be stored on **designated drives and servers,** and should only be uploaded to **approved cloud services.**
- Servers containing personal data should be **sited in a secure location**, away from general office space. This is true for both HQ and field offices.
- Data should be **backed up frequently.** Those backups should be tested regularly, in line with Dorcas's standard backup procedures.
- Data should **never be stored** to local hard drives, laptops or other mobile devices like tablets or smart phones. If for some reason it is temporarily necessary to transport data on a laptop, please refer to what has been said about data stored on removable media.
- All servers containing data and all 'clients' (laptops, desktops and thin clients) should be protected by **approved security software and a firewall.**

5. Data use

Personal data is of no value to Dorcas, unless it can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Therefore:

- When working with personal data (think of CRM, Twinfield, Cobra, etc.), employees should ensure the **screens of their computers are always locked** when left unattended.

- Personal data **should not be shared informally.** In particular, it should never be sent by email, as this form of communication is not secure. This particularly applies to sending scans of passports by e-mail.
- Personal data must be **encrypted before being transferred electronically.** The IT coordinator will provide means to do this and can explain how to send data in this manner to authorized external contacts.
- Remote access to servers at HQ can **only be made through VPN** (Virtual Private Network) with proper authentication.
- Personal data of people within the European Economic Area **should not be stored or transferred outside of the European Economic Area.**
- Employees should not **save copies of personal data to their own computers.** Always access and update the central copy of any data.

6. Data accuracy

The law requires Dorcas to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Dorcas should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary.** Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure **data is updated.** For instance, by confirming a customer's details when they call.
- Dorcas will make it **easy and safe to update the information** for 'data subjects' that Dorcas holds about them, for instance via the company website.
- Data should be **updated as inaccuracies are discovered.** For instance, if a supporter or volunteer can no longer be reached on their stored telephone number, it should be removed from the database; or if snail mail is returned, the address should be either deleted or marked as inaccurate in the database.
- It is the team leaders Private Donor's responsibility to ensure **marketing databases are checked against industry suppression files** (to check for obsolete and redundant addresses) whenever it is deemed necessary.

7. Subject access requests

All individuals, companies or organizations who are the subject of personal data held by Dorcas are entitled to:

- Ask **what information** Dorcas holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations.**

If an individual, company or organization contacts Dorcas requesting this information, this is called a ´subject access request´.

Subject access request should be made by e-mail, addressed to info@dorcas.nl or alternatively by mail to Post Office Box 12, 1619 ZG Andijk, or by telephone through the receptionist at +31 228 59 59 00. The team leader Back Office will handle the request and will make sure the requesting party is appropriately answered by providing the relevant data within 14 days, after the identity of the requesting individual, company or organization has been established.

8. Disclosing data for other reasons

In certain circumstances, the Law on Protection of Personal Information or other Dutch or foreign legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Dorcas will disclose requested data. However, the director of finance and supporting services will ensure the request is legitimate, seeking assistance from the board and where necessary form legal advisers where necessary.

If Dutch law is not in accordance with foreign law, especially when compared with legislation of the United States of America, Dutch law prevails to determine whether information will be disclosed.

9. Providing information

Dorcas aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, Dorcas has a privacy statement for the Dutch setting, spelling out how data relating to individuals is used by Dorcas. This statement is attached to this policy.

10. Beneficiary's rights

Everything that is stipulated in this policy, is also applicable for data that Dorcas needs and collects of beneficiaries, in the context of the implementation of the Dorcas programs. The same precautions must be taken with beneficiary data as with all other individual data information. Moreover, there are additional privacy guidelines that Dorcas adheres to when it comes to privacy rights of beneficiaries, which are in the process of being put down in Dorcas privacy guidelines for beneficiaries, which includes stipulations about consent for use of photographic material, not using information and photographs outside of the context, guarding the dignity of beneficiaries and appropriate use of information.

Enclosure 1 – Privacy Statement

Persoonsgegevens die Dorcas verzamelt, gebruikt Dorcas alleen voor het doel waarmee je ze aan Dorcas hebt gegeven. Daarmee voldoet Dorcas aan de privacywetgeving.

Wat zijn persoonsgegevens?

Een persoonsgegeven is informatie die herleidbaar is tot een persoon. Voorbeeld van een persoonsgegeven is een naam of een huisadres, maar ook e-mailadressen kunnen persoonsgegevens zijn.

Vastleggen en verwerken van gegevens

Daar waar jouw persoonsgegevens verwerkt worden, staat precies vermeld welke gegevens voor welke doeleinden gebruikt worden. Dorcas gebruikt je persoonsgegevens enkel voor het doel waarvoor je ze hebt gegeven. We garanderen dat je gegevens niet worden gebruikt voor andere doelen dan voor informatieverstrekking en betrokkenheid bij de projecten van Dorcas. Het betekent ook dat Dorcas je gegevens niet gebruikt voor andere doeleinden dan voor deze doeleinden. Dorcas zal nimmer adressen verkopen of beschikbaar stellen aan derde partijen.

Persoonsgegevens worden niet langer bewaard dan nodig is voor het doel waarvoor de gegevens gevraagd zijn. Door het beschikbaar stellen van je gegevens, geef je ons toestemming om je persoonlijke gegevens op te slaan in onze database en die te gebruiken voor het doel waarvoor je deze aan ons hebt gegeven. Deze toestemming en bewaartermijn zijn vastgelegd in het Vrijstellingsbesluit Wet Bescherming Persoonsgegevens.

Voor alle verwerkingen van persoonsgegevens geldt dat alleen die gegevens worden gebruikt, die je zelf hebt achtergelaten. De achtergelaten gegevens worden vertrouwelijk behandeld. De persoonlijke gegevens worden alleen vrijgegeven met jouw uitdrukkelijke toestemming. Jouw persoonlijke gegevens stellen we niet aan derden beschikbaar, tenzij we dit op grond van de wet verplicht zijn.

Dorcas kan vragen om je locatiegegevens op mobiele apparaten. Deze gegevens worden dan allen gebruikt om je zo goed mogelijk van dienst te zijn bij het verstrekken van informatie. Deze gegevens worden alleen gebruikt wanneer je hier toestemming voor hebt gegeven.

Je bepaalt zelf welke gegevens aan wie ter beschikking worden gesteld. Als er zogenaamde profielen worden bijgehouden, dan worden die uitsluitend gebruikt om de website beter af te stemmen op de behoefte van de gebruiker en wordt dat van te voren meegedeeld.

Gegevens kunnen echter wel worden gebruikt voor opsporing, als strafbare feiten worden gepleegd of strafbare uitlatingen worden gedaan (en verdere uitzonderingen zoals genoemd in art. 43 WBP). Als je jouw gegevens wilt inzien, laten corrigeren of verwijderen, dan kun je een verzoek bij ons indienen door een e-mail te sturen naar info@dorcas.nl